REMARKS

STATUS OF THE CLAIMS

Claims 1, 3, and 5-18 are pending in the application.

Claims 1, 3, 5-7, 9, 12-14, 17, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deo et al. (U.S. 5,721,781) in view of Niwata et al. (U.S. 6,595,415).

Claims 8, 10, 11, 15, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deo et al. (U.S. 5,721,781) as modified by Niwat et al. (U.S. 6,595,415) as applied to claims 1, 13, and 14 above, and further in view of LeBourgeois (U.S. 6,026,166).

Thus, pending claims remain pending for reconsideration, which is respectfully requested.

No new matter has been added.

REJECTIONS

Claims 1, 3, 5-7, 9, 12-14, 17 and 18 are rejected under 35 USC 103(a) as being unpatentable over Deo (US Patent No. 5,721,781) in view of Niwata (US Patent No. 6,595,415). Niwata is newly cited, and, thus, newly relied upon.

Claims 8, 10, 11, 15 and 16 are rejected under 35 USC 103(a) as being unpatentable over Deo, Niwata and LeBourgeois (US Patent No. 6,026,166).

The independent claims are 1, 13, 14, 17 and 18, which are rejected over Deo and Niwata.

The Office Action newly relies on Niwata to meet the claimed present invention's "***a plurality of identification conditions including identification means and identification levels that are selectable for use;*** and means for ***selecting one of the plural identification conditions to perform identification, according to identification condition setting information received from a server every time a request for identification is received from the server.***"

The Office Action relies on Niwata's FIG. 16 and column 21, lines 66+, which discuss acquiring card information corresponding to security level (FIG. 17, SJ6). In other words, Niwata

FIGS. 16-17 and column 22, lines 18-60 discuss when the IC card 20 is inserted in the card inlet 42 of the IC card processor 40, apparatus side security code and the security level setting information are read from the IC card 20 and stored or written in the nonvolatile memory 59 of the IC card processor 40 (column 12, lines 17-38 and FIG. 16, SJ3). Then, the IC card processor 40 refers to the apparatus side security code and security level written in the nonvolatile memory 59 of the IC card processor 40 to acquire information from the IC card 20 depending on the security level. For example, if the security level is 2 (see FIG. 16) only the name information is read from the IC card 20 and displayed by the IC card processor. Therefore, Niwata's security level is usable to control confidentiality of information stored on the IC card 20 (column 24, lines 57-62).

However, Niwata protects confidentiality of information stored on the IC card 20, but the claimed present invention provides "***selecting ... identification conditions to perform identification, according to identification condition setting information received from a server every time a request for identification is received from the server***." In other words, the claimed present invention's identification (or authentication) by performing "***identification according to identification condition setting information***" differs from protecting information confidentiality. Identification or authentication relates to identifying a person. For example, the present application FIG. 1, identification information storing portion 15 of terminal 1, and page 8, lines 17-23; page 10, line 1 to page 11, line 8, support the claimed present invention.

Niwata does not provide any motivation to one skilled in the art to modify Deo to provide authentication as claimed, thus, a prima facie case of obviousness over Deo and Niwata has not been established.

Further, even if one interpreted Deo's ATM terminal 32 as a server, as suggested by the Office Action page 3, Deo's ATM terminal 32 does not receive any "***identification condition setting information***" from another server to instruct the ATM machine 32 to perform identification or authentication with a smart card based upon the received "***identification condition setting information***" and the ATM terminal 32 does not provide any identification condition setting information to the smart card 10, since Deo column 11 and FIG. 9, relied upon by the Office Action, discuss a smart card determining a type of terminal and selecting a security level based upon the type of terminal.

Further, Niwata fails to disclose or suggest to one skilled in the art to modify Deo to provide the claimed present invention's "***sending to the server, as a confirmation, identification condition used by the personal identification terminal for the identification, in a format enabling detection of an alteration thereof, together with a result of the identification***," because neither Deo or Niwata discuss a terminal confirming to a server that the terminal performed an identification, or authenticated a user, as set or instructed by the server. In other words, the limitation as recited in independent claims 1, 14, and 17, that is, a structure in which the terminal sends back to the server, as confirmation, identification condition (an identification means and an identification level) that was used actually by the terminal, in a format enabling detection of an alteration thereof, together with a result of the identification, is not disclosed or suggested anywhere in the cited references. A prima facie case of obviousness cannot be established based upon Deo, Niwat and LeBourgeois, because Deo column 11 and FIG. 9 discuss a smart card determining a type of terminal and selecting a security level based upon the type of terminal, Niwata protects confidentiality of information stored on the IC card 20, and LeBourgeois is relied upon for discussing providing a level of authentication confidence, all of which fail to disclose or suggest the claimed present invention's terminal sending to a server identification condition (an identification means and an identification level) that was used actually by the terminal, and in a format enabling detection of an alteration thereof, together with a result of the identification. The claimed present invention provides a new non-obvious effect of allowing a server to confidently confirm that a terminal performed identification according to the server's "***identification condition information setting***" sent to the terminal, by (1) the server sending such identification condition setting information to the terminal and by (2) the server detecting any alteration of a confirmation of actual identification condition used by the terminal.

Accordingly, it is believed the claimed present invention is allowable over Deo, Niwat and LeBourgeois.

Further, the Office Action page 4, line 4, provides "it would have been obvious to an ordinary skill in the art at the time the invention was made to incorporate well known security setting means to the teachings of Deo ..." To the extent the Examiner alleges the authentication or identification setting as claimed is well known, the Applicant respectfully traverses the Examiner's statement and demands the Examiner produce authority for the statement. The Applicant specifically points out the following errors in the Examiner's action.

First, the Examiner appears to use common knowledge as the principal evidence for the assertion that identification setting as claimed is well known. As explained in M.P.E.P. §2144.03(E):

> any facts so noticed should . . . serve only to 'fill in the gaps' in an insubstantial manner which might exist in the evidentiary showing made by the Examiner to support a particular ground of rejection. It is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection was based.

Second, the noticed fact is not considered to be common knowledge or well-known in the art, because in this case, the claimed limitations concerning personal identification setting or authentication setting is not of notorious character or capable of instant and unquestionable demonstration as being well-known. Instead, the limitations as claimed are unique to the present invention. In contrast to Deo, Niwat and LeBourgeois, the claimed present invention provides:

> 1. (PREVIOUSLY PRESENTED) A personal ***identification terminal*** comprising:
>
> a plurality of ***identification conditions including identification means and identification levels*** that are selectable for use; and
>
> means for ***selecting one of the plural identification conditions to perform identification***, according to ***identification condition setting information received from a server every time a request for identification is received from the server***,
>
> wherein the identification condition setting information received from the server includes a digital signature for detecting an alteration thereof; and
>
> means for ***sending to the server, as a confirmation, identification condition used by the personal identification terminal for the identification, in a format enabling detection of an alteration thereof, together with a result of the identification*** (emphasis added).

See M.P.E.P. §2144.03(A) - " ... the notice of facts beyond the record which may be taken by the Examiner must be 'capable of such instant and unquestionable demonstration as to defy dispute' ... "

Third, there is no evidence supporting the Examiner's assertion, because Niwata

discusses information confidentiality and the present invention provides personal identification setting or authentication setting as claimed. And the Office Action page 3 acknowledges that Deo does not discuss the claimed present invention's "***selecting one of the plural identification conditions to perform identification***, according to ***identification condition setting information received from a server every time a request for identification is received from the server*** ... ***and*** ... ***sending to the server, as a confirmation, identification condition used by the personal identification terminal for the identification, in a format enabling detection of an alteration thereof, together with a result of the identification***." See M.P.E.P. §2144.03(B) ("there must be some form of evidence in the record to support an assertion of common knowledge").

Fourth, to the extent the Examiner bases the rejection, at least in part, on personal knowledge, the Examiner is required under 37 C.F.R. §1.104(d)(2) to support such an assertion with an affidavit when called for by the Applicant. Thus, Applicant calls upon the Examiner to support any such assertion with an affidavit.

INDEPENDENT CLAIM 13

Further, independent claim 13 is patentable over Deo, Niwata and LeBourgeois, because the Office Action does not provide a rejection rationale for the claimed limitation that a result of the identification and a score, which is a similarity of biometric identification, is sent from the terminal to the server, if biometric identification is performed by the terminal (i.e., claim 13 provides: "storing a log of ***a score that indicates a similarity, if the personal identification terminal performed the identification using biometric information***, or a hash value of the score, that was ***added to result information of the identification received from the personal identification terminal according to the sending of the identification condition setting information***"). Then, the server can decide whether the identification failed when, for example, the same score value continues several times despite the result of the identification. For example, the present Application FIG. 4 and page 14, lines 21+ support independent claim 13.

The Office Action page 5 relies on LeBourgeois column 4, lines 7-27 and column 9, lines 29-57, which discuss providing a level of confidence using a challenge code or "obtains data regarding listed components present in user system" FIG. 4, step 416. LeBourgeois column 12, lines 3+ discuss authorizing based upon whether the difference between the original signature

and the real-time signature exceeds some predetermined threshold. However, LeBourgeois confidence levels fail to disclose or suggest to one skilled in the art the claimed present invention's confidence level determination of "***failing the identification, if same score value continues several times in accordance with the read log of the score*** or the hash value of the score, ***despite a result of the identification received from the personal identification terminal***." For example, LeBourgeois is silent on any confidence level based upon logging of identification scores.

Further, contrary to the Office Action suggestion, LeBourgeois dependent claim 2 appears to include a typographical error in which the phrase "scoring" is intended to be "storing," because claim 1 does not recite a "scoring" limitation.

LeBourgeois fails to disclose, either expressly or inherently, or suggest to one skilled in the art, the claimed present invention's confidence level determination as claimed in independent claim 13.

In view of the remarks, it is believed the claims are allowable over the relied upon references and withdrawal of the rejection of pending is respectfully requested.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: July 5, 2006

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501